

ATTACHMENT C

AFFIDAVIT of
Special Agent Ryan Temm
Bureau of Alcohol, Tobacco, Firearms and Explosives
Bristol, Virginia

1. I, Special Agent Ryan Temm, being duly sworn hereby depose and say:
2. I am a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been employed for approximately eight (8) years. I received my training at the Federal Law Enforcement Training Center (FLETC), and ATF National Academy in Brunswick, Georgia. At the ATF National Academy we trained in various investigative techniques to include preparing a proper search warrant. During my time at the ATF, I have been trained in the investigation of violations of numerous federal criminal statutes. Since becoming a Special Agent with ATF, I have participated in numerous search and arrest warrants. I have a Bachelor of Arts Degree in Criminal Justice from The George Washington University and a Master of Public Administration from the University of North Carolina at Charlotte. I successfully completed a basic law enforcement academy with the Charlotte-Mecklenburg Police Department and served nearly eight years as a police officer.
3. I have also consulted in this investigation with Gregory Watson, Senior Special Agent (SSA) of the U. S. Secret Service (USSS). He has been so employed since June of 2000 and has been in law enforcement since March 1998. While employed by the USSS, he has investigated federal criminal violations related to high technology or cyber-crime, child exploitation, and child pornography. He has observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in many forms of media including computer and cell phone media.
4. The facts set forth in this affidavit are known to me as a result of my personal participation and information provided to me by other law enforcement personnel involved in this investigation.
5. This affidavit is being submitted for the limited purpose of obtaining a search warrant for the items listed in Attachment B, it is not intended to include each and every fact observed by myself, other involved law enforcement officers or deputies or known to the government. I have set forth only those facts necessary to support probable cause for this application.
6. This affidavit is submitted pursuant to Rule 41 of the Federal Rules of Criminal Procedure in support of an application for a warrant authorizing the search of the electronic devices (hereinafter referred to as the "Target Electronic Media") seized during the execution of a Federal Search Warrant on October 5, 2016, at 8615 Hubbard

Mountain Road, Pound, Virginia for the items specified in Attachment B. I have probable cause to believe that evidence of a crime, fruits of a crime, contraband and instrumentalities of a violation of: 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), are located in the devices which are located in the Western District of Virginia. Located within the devices to be searched, I seek to seize evidence, fruits and instrumentalities of the foregoing criminal violation. I request authority to search the entirety of the devices as described in Attachment A.

7. In summary, this affidavit sets forth facts that establish that there is probable cause to believe the devices possessed by David MATHIAS at 8615 Hubbard Mountain Road, Pound, Virginia, contain evidence of this crime. These devices were seized during the execution of a Federal Search Warrant on October 5, 2016, at 8615 Hubbard Mountain Road, Pound, Virginia.

RELEVANT STATUTE

This investigation concerns an alleged violation of 18 U.S.C § 2252A(a)(5)(B) (possession of child pornography). 18 U.S.C § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

1. The following definitions apply to this Affidavit:
 - a. "Child erotica," as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
 - b. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - c. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any

data storage facility or communications facility directly related to or operating in conjunction with such device.”

- d. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A DNS (domain name system) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.google.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.
- e. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- f. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- g. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- h. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- i. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- j. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- k. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.
- l. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- m. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).
- n. "Peer-to-peer file-sharing" ("P2P") is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.
- o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether

in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi-Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).
- q. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).
- r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

1. Computers and digital technology have revolutionized the way in which individuals interested in child pornography interact with one another. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.
2. The development of computers and digital cameras has changed this. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.
3. Individuals who access with intent to view and/or possess, receive, distribute or advertise child pornography can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when

the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store over 100 gigabytes of data, which provide enough space to store thousands of high-resolution photographs. Video camcorders that once recorded video onto tapes or mini-CDs can now save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

4. A device known as a modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
5. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One terabyte (1000 gigabytes) external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them.)
6. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

7. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

PEER TO PEER (P2P) FILE-SHARING

8. A growing phenomenon on the Internet is peer-to-peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using P2P software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files currently being shared on the network. BitTorrent, one type of P2P software, sets up its searches using keywords. The results of a keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the file.
9. For example, a person interested in obtaining child pornographic images would open the P2P application on his/ her computer and would conduct a keyword search for files using a term such as "pre-teen sex." That keyword search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the file(s) he or she wants to download. Selected files are downloaded directly from the computer sharing the file. The downloaded file is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.
10. P2P file-sharing allows individuals to meet each other through the Internet, engage in social networking, and trade files. One aspect of P2P file-sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.
11. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address identifies the location of the

computer with which the address is associated, making it possible for data to be transferred between computers. Third-party software is available to identify the IP address of the P2P computer sending a file. Such software monitors and logs Internet and local network traffic.

12. Files being shared by users on a P2P network are processed by the user's P2P software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The user's P2P software succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

1. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:
 - a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
 - b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a

computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

2. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).
3. Furthermore, because there is probable cause to believe that the computers and their storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

1. The first step in the forensic computer data examination process is to make an exact copy of the data subject to the examination. The forensic examination is performed on the copy of the data to eliminate the chance of damaging any original data in the exam process. In an exam for sexually explicit material involving minors, computer forensic analysis software is then used to screen all of the data for files that contain specific characteristics of child pornography and sexually explicit material involving minors such as graphic files, picture files, still image files, and video files. The computer forensic analysis software highlights these files for more detailed review by the forensic examiner. The examiner then carefully reviews these selected files as described in paragraph 3 (this page) above.
2. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise

unlawfully possessed, or (5) evidence of the offenses specified above);

- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

1. *Forensic evidence:* As further described in Attachment B, this application seeks permission to locate not only computer files, audio files, video files, documents, IP logs, phone records, text messages, and other data files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Target Electronic Media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Target Electronic Media because:
 - a. Data on a computer storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
 - b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the

data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
2. *Necessity of seizing or copying entire computer or storage media:* A thorough search of the Target Electronic Media requires the seizure of the Target Electronic Media and later off-site review consistent with the warrant. This is true because of the following:
- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the Target Electronic Media to obtain evidence. Such storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
 - b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data. However, taking the computer storage media off-site and reviewing it in an environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
3. *Nature of examination:* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media on the Target Electronic Media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.
4. *Manner of Execution:* Because this warrant seeks only permission to examine the Target Electronic Media, all of which is already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

PROBABLE CAUSE

1. On October 5, 2016, a Federal Search Warrant was executed at the residence of David MATHIAS and Stephany Mullins (Mathias), 8615 Hubbard Mountain Road, Pound, VA, for violations of Title 21 USC 841 and 846, Distribution of a Controlled Substance and Conspiracy to Distribute a Controlled Substance. During the search of the premises a number of items were seized pursuant to the search warrant. Among these items were several items of electronic evidence including: HP, model 2000-2b09wm, S/N: 5CG23703VG laptop computer (ATF evidence item #00091), HP, model 2000-2b19wm, S/N: 5CG30532HT laptop computer (ATF evidence item #00092), Dell, model Inspiron N5050, S/N: DH5JLT1 laptop computer (ATF evidence item #00093) and a Samsung, SCH-I545BLK, IMEI 990003433923048, cellular telephone (ATF evidence item #00096).
2. The three laptop computers were taken from the master bedroom. The two HP computers were found stacked on top of one another in the drawer of the nightstand next to the bed. On top of this nightstand was a cellphone believed to belong to David MATHIAS. A \$100 bill among other US currency, determined to have been used by the DTF as buy money on the previous night's synthetic cannabinoid controlled purchase, was also on the nightstand. The Dell computer was on a small desk in the corner of the bedroom opposite the bed. The Samsung telephone was taken from the drawer of the end table in the living room. The table was at the end of the sofa. The phone did not have a battery. The day prior to the search MATHIAS had contacted the Confidential Informant (CI) and told him his old phone was no longer working and that he had a new phone number. When I turned this Samsung phone on a spoof FBI warning banner came up stating that

due to the user visiting certain illicit (pornography) web sites the phone had been locked, but could be unlocked after paying a fine. Due to the contents (contacts, call history etc.) of this phone I believe it to belong to David MATHIAS.

3. On October 6, 2016, I began the digital forensic exam of the items taken from 8615 Hubbard Mountain Road. I am a certified Digital Media Collection Specialist (DMCS). Regarding the Samsung, model SCH-I545BLK, IMEI 990003433923048, cellular telephone, the data was extracted using Cellebrite's Universal Forensic Extraction Device (UFED) 4PC (V. 5.3.0.731). Extracted data was viewed using UFED Physical Analyzer (V. 5.3.5.14). A preliminary forensic examination of the cellular telephone seized from 8615 Hubbard Mountain Road, revealed numerous images of apparent child pornography as defined in 18 U.S.C. § 2256.
4. The UFED Physical Analyzer parsed out 22,605 images extracted from the Samsung, model SCH-I545BLK, I personally reviewed approximately 10,000 of the images and viewed what I believe to be approximately, at least, 50 images of child pornography. Also of note there were hundreds of images of bestiality, persons engaged in sex acts with animals.
5. On November 10, 2016 USSS SSA Greg Watson viewed a number of the images I believed to be depictions of child pornography and he agreed with my assessment, the images did indeed depict child pornography.

Conclusion

Based upon the foregoing, I submit that there is probable cause to believe that the property described in Attachment A, contains evidence, contraband, fruits and instrumentalities pertaining to a violation of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography)

I, therefore, respectfully request that the attached search warrant be issued authorizing the search of property described in Attachment A.

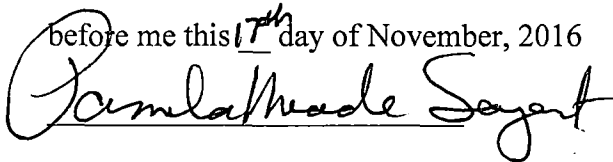


Ryan C. Temm
Special Agent

Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn

before me this 17th day of November, 2016



Pamela Meade Sargent
United States Magistrate Judge